确定在Firepower威胁防御(FTD)上运行的活动Snort版本

目录

简介

本文档介绍在思科Firepower设备管理器(FDM)、思科Firepower管理中心(FMC)或思科防御协调器(CDO)管理思科Firepower威胁防御(FTD)时，确认运行活动Snort版本的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Firepower管理中心(FMC)
- 思科Firepower威胁防御(FTD)
- 思科Firepower设备管理器(FDM)
- 思科防御协调器(CDO)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Firepower威胁防御(FTD)v6.7.0和7.0.0
- 思科Firepower管理中心(FMC)v6.7.0和7.0.0
- 思科防御协调器(CDO)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

SNORT®入侵防御系统正式推出了Snort 3全面升级，该升级具有提高性能、加快处理速度、提高网络可扩展性等改进功能和新功能，并且具有200多个插件，因此用户可以为其网络创建自定义设置。

Snort 3的优势包括（但不限于）：

- 性能改善
- 改进的SMBv2检测
- 新的脚本检测功能
- HTTP/2检测
- 自定义规则组
- 使自定义入侵规则更易于编写的语法
- 入侵事件中“本应已丢弃”内联结果的原因
- 当更改部署到VDB、SSL策略、自定义应用检测器、强制网络门户身份源和TLS服务器身份发现时，不重新启动Snort
- 通过向Cisco Success Network发送特定于Snort 3的遥测数据，以及更好的故障排除日志，提高了可维护性

对Snort 3.0的支持是针对6.7.0 Cisco Firepower威胁防御(FTD)引入的，这时正是FTD通过Cisco Firepower设备管理器(FDM)进行管理的时候。

注：对于由FDM管理的新6.7.0 FTD部署，Snort 3.0是默认检测引擎。如果您将FTD从较旧版本升级到6.7，则Snort 2.0仍为活动检测引擎，但您可以切换到Snort 3.0。

注意：对于此版本，Snort 3.0不支持虚拟路由器、基于时间的访问控制规则或TLS 1.1或更低连接的解密。仅在不需要这些功能时启用Snort 3.0。

然后，Firepower版本7.0引入了对由Cisco FDM和Cisco Firepower管理中心(FMC)管理的Firepower威胁防御设备的Snort 3.0支持。

注意：对于新的7.0 FTD部署，Snort 3现在成为默认检测引擎。升级后的部署继续使用Snort 2，但您可以随时进行切换。

注意：您可以在Snort 2.0和3.0之间自由切换，以便根据需要恢复更改。只要您切换了版本，流量就会中断。

⚠ 注意：在切换到Snort 3之前，强烈建议您阅读并理解《Firepower管理中心Snort 3配置指南》。请特别注意功能限制和迁移说明。虽然升级到Snort 3是为了将影响降至最低，但功能并不完全匹配。升级前的规划和准备工作可以帮助您确保按照预期处理流量。

确定在FTD上运行的活动Snort版本

FTD命令行界面(CLI)

要确定在FTD上运行的活动snort版本，请登录到FTD CLI并运行show snort3 status命令：

示例1:当未显示输出时，FTD运行Snort 2。

```
<#root>

>

show snort3 status

>
```

示例2:当输出显示“Currently running Snort 2”时,FTD将运行Snort 2。

```
<#root>

>

show snort3 status

Currently running Snort 2
```

示例3:当输出显示“Currently running Snort 3”时，FTD运行Snort 3。

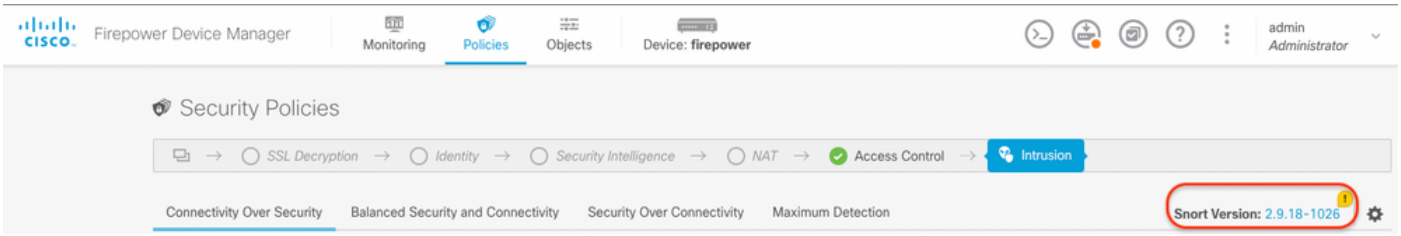
```
<#root>

>

show snort3 status

Currently running Snort 3
```

由Cisco FDM管理的FTD

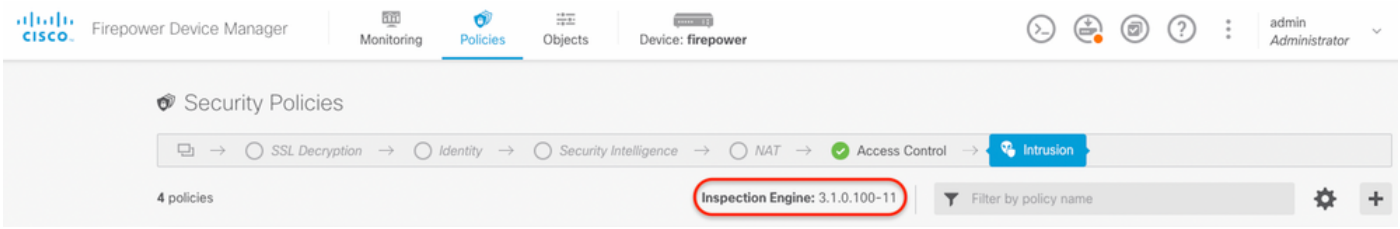
要确定在Cisco FDM管理的FTD上运行的活动Snort版本，请继续执行以下步骤：

1. 通过FDM Web界面登录思科FTD。
2. 从主菜单中选择Policies。
3. 然后，选择Intrusion选项卡。
4. 查找Snort Version或Inspection Engine部分以确认FTD中处于活动状态的Snort版本。

示例1:FTD运行snort版本2。



示例2:FTD运行snort版本3。

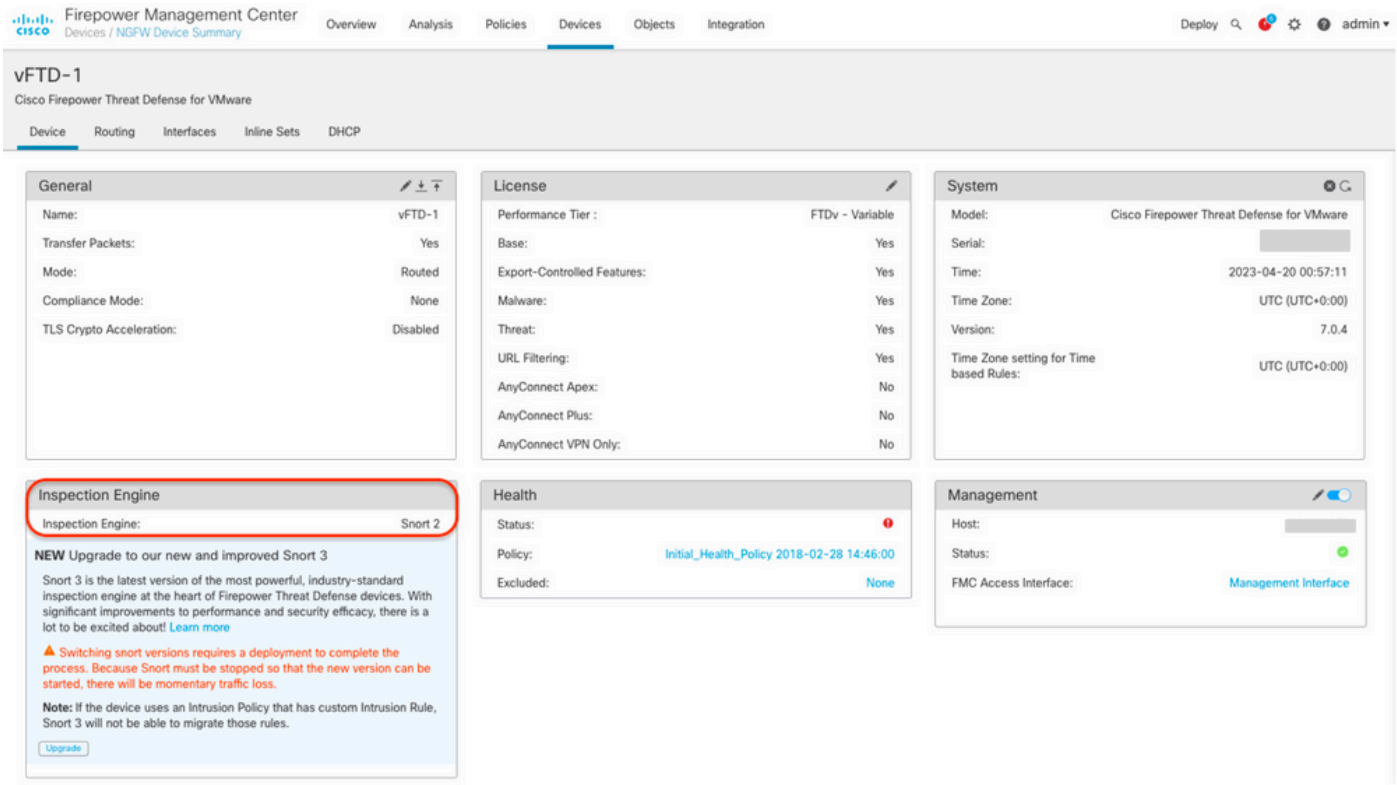


由管理的FTD 思科FMC

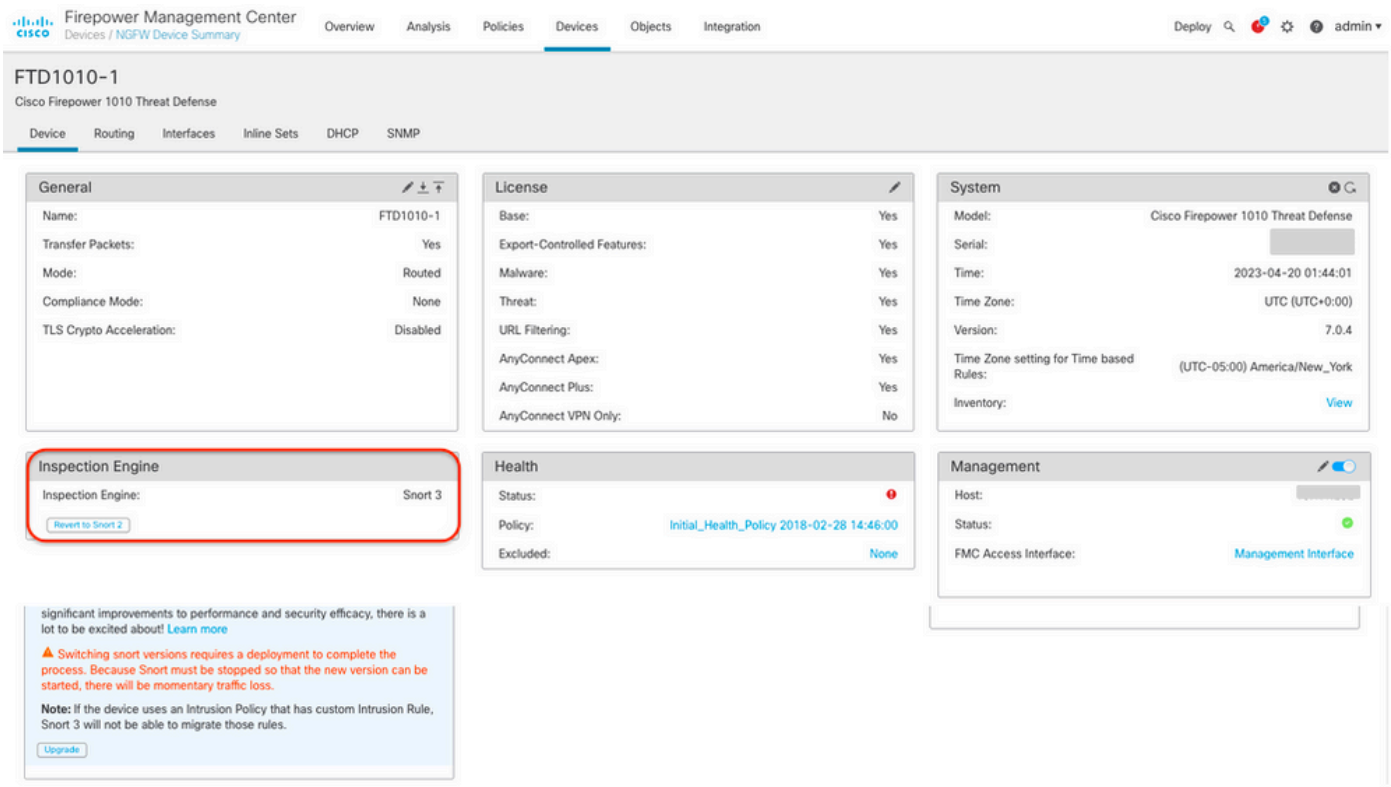
要确定在Cisco FMC管理的FTD上运行的活动Snort版本，请继续执行以下步骤：

1. 登录到Cisco FMC Web界面。
2. 从Devices菜单中选择Device Management。
3. 然后，选择适当的FTD设备。
4. 单击Edit铅笔图标。
5. 选择Device选项卡并查找Inspection Engine部分以确认FTD中处于活动状态的snort版本：

示例1:FTD运行snort版本2。



示例2:FTD运行snort版本3。



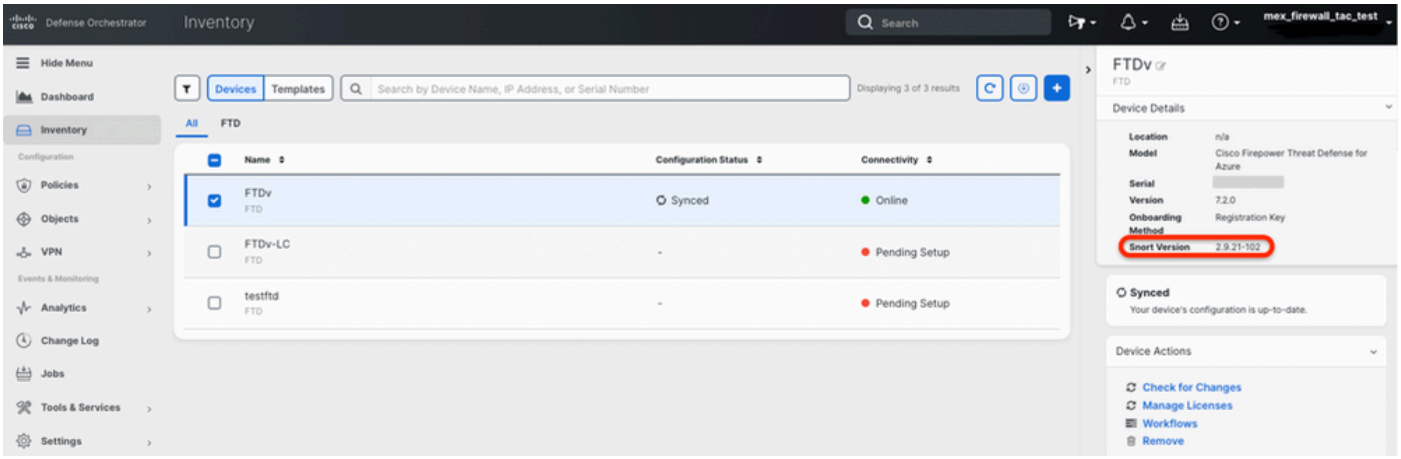
由管理的FTD 思科CDO

要确定在Cisco Defense Orchestrator管理的FTD上运行的活动Snort版本，请继续执行以下步骤：

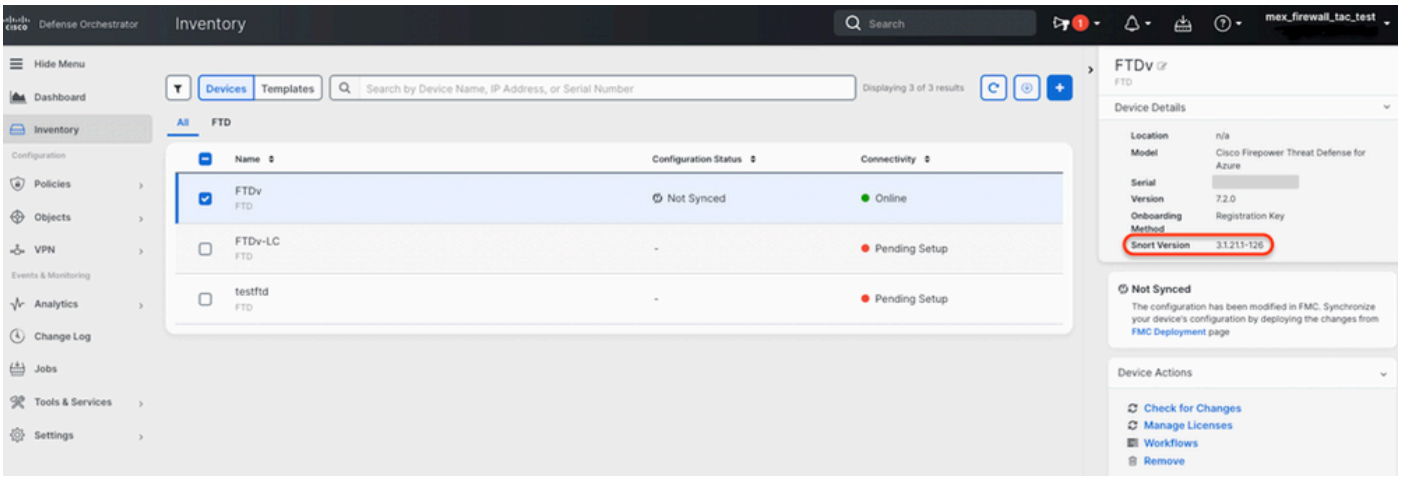
1. 登录到Cisco Defense Orchestrator Web界面。

2. 从Inventory菜单中，选择适当的FTD设备。
3. 在Device Details部分中，查找Snort Version:

示例1:FTD运行snort版本2。



示例2:FTD运行snort版本3。



相关信息

- 思科Firepower版本说明，版本6.7.0
- 思科Firepower版本说明，版本7.0
- Snort 3网站
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。